Coefficients of cyclotomic polynomials

Pingzhi Yuan
School of Mathematics, South China Normal University , Guangzhou 510631, P.R.CHINA
e-mail mcsypz@mail.sysu.edu.cn

Abstract

Let $a(n,k)$ be the k-th coefficient of the n-th cyclotomic polynomial. Recently, Ji, Li and Moree [12] proved that for any integer $m \geq 1$, $\{a(mn,k)|n,k \in \mathbb{N}\} = \mathbb{Z}$. In this paper, we improve this result and prove that for any integers $s > t \geq 0$,

$$\{a(ns+t,k)|n,k \in \mathbb{N}\} = \mathbb{Z}.$$

2000 Mathematics Subject Classification:11B83; 11C08
Keywords: Cyclotomic polynomials; Dirichlet's theorem; Squarefree integers

1 Introduction

Let $\Phi_n(x) = \sum_{k=0}^{\varphi(n)} a(n,k)x^k$ be the nth cyclotomic polynomial. The Taylor series of $1/\Phi_n(x)$ around $x = 0$ is given by $1/\Phi_n(x) = \sum_{k=0}^{\varphi(n)} c(n,k)x^k$. It is not difficult to show that $a(n,k)$ and $c(n,k)$ are all integers. The coefficients $a(n,k)$ and $c(n,k)$ are quite small in absolute value, for example for $n < 105$ it is well-known that $|a(n,k)| \leq 1$ and for $n < 561$ we have $|c(n,k)| \leq 1$(see [13]). Migotti [8] showed that all $a(pq,i) \in \{0,\pm1\}$, where p and q are distinct primes. Beiter [3] and [4] gave a criterion on i for $a(pq,i)$ to be $0,1$ or -1, see also Lam and Leung [6]. Also Carlitz [5] computed the number of non-zero $a(pq,i)$'s. For more information on this topic, we refer to the beautiful survey paper of Thangadurai [14]. Bachman [1, 2] proved the existence of an infinite family of $n = pqr$ with all $a(pqr,i) \in \{0,\pm1\}$, where p,q,r are distinct odd primes.

Let $m \geq 1$ be a integer. Put

$$S(m) = \{a(mn, k)|n \geq 1, k \geq 0\} \quad \text{and} \quad R(m) = \{c(mn, k)|n \geq 1, k \geq 0\}.$$

Schur poved in 1931 (in a letter to E. Landau) that $S(1)$ is not a finite set, see Lenstra [7]. In 1987 Suzuki [10] proved that $S(1) = \mathbb{Z}$. Recently, Ji, Li and Moree [12], [11] proved that with $S(m) = R(m) = \mathbb{Z}$ for any integer $m \geq 1$.

Let $m \geq 1, s > t \geq 0$ be positive integers with $\gcd(s, t) = 1$. Put

$$S(m; s, t) = \{a(m(sn+t), k)|n \geq 1, k \geq 0\} \quad \text{and} \quad R(m; s, t) = \{c(m(sn+t), k)|n \geq 1, k \geq 0\}.$$

In this note, by a slight modification of the proof in [12], we prove the following generalization of the result in [12].

Theorem 1.1. *Let $m \geq 1, s > t \geq 0$ be positive integers with $\gcd(s, t) = 1$. Then $S(m; r, t) = R(m; s, t) = \mathbb{Z}$.*

An equivalent statement of Theorem 1.1 is the following result, which is the motivation to write this paper.

Theorem 1.2. *Let $s > t \geq 0$ be integers, then*

$$\{a(ns + t, k)|n, k \in \mathbb{N}\} = \{c(ns + t, k)|n, k \in \mathbb{N}\} = \mathbb{Z}.$$

2 Some Lemmas

Lemma 2.1. ([12] Lemma 1) *The coefficient $c(n, k)$ is an integer whose value only depends on the congruence class of k modulo n.*

Let $\kappa(m) = \prod_{p|m} p$ denote the squarefree kernel of m.

Lemma 2.2. ([12] Corollary 1) *We have $S(m) = S(\kappa(m))$ and $R(m) = R(\kappa(m))$.*

Lemma 2.3. (Quantitative Form of Dirichlets Theorem) *Let a and m be coprime natural numbers and let $\pi(x; m, a)$ denote the number of primes $p \leq x$ that satisfy $p \equiv a \pmod m$. Then, as x tends to infinity,*

$$\pi(x; m, a) \sim \frac{x}{\varphi(m) \log x},$$

where ϕ is Euler's toitent function.

Lemma 2.4. ([12] Corollary 2) *Given $m, t \geq 1$ and any real number $r > 1$, there exists a constant $N_0(t, m, r)$ such that for every $n > N_0(t, m, r)$ the interval (n, rn) contains at least t primes $p \equiv 1 \pmod m$.*

3 The proof of Theorem 1

Proof. We first prove that $S(m;s,t)=\mathbb{Z}$. Since $S(m;s,t)=S(\kappa(m);s,t)$ and $S(m;s,t)\supseteq S(mp;s,t)$, where $p\equiv 1 \pmod s$ is an odd prime, we may assume that m is square-free, $m>1$ and $\mu(m)=1$. Suppose that $n>N_0(t,ms,\frac{15}{8})$, then, by Lemma 2.4, there exist primes $p_1,p_2,\dots,p_t$ such that

$$N<p_1<p_2<\cdots<p_t<\frac{15}{8}n \quad \text{and} \quad p_j\equiv 1 \pmod{ms}, \quad j=1,2,\dots,t.$$

Let q_1,q_2 be primes such that $q_2>q_1>2p_1$, $q_1\equiv t \pmod s$ and $q_2\equiv 1 \pmod s$ and put

$$m_1=\begin{cases} p_1p_2\cdots p_tq_1 & \text{if } t \text{ is even;}\\ p_1p_2\cdots p_tq_1q_2 & \text{otherwise.}\end{cases} \tag{1}$$

Note that m and m_1 are coprime, $m_1\equiv t \pmod s$ and that $\mu(m_1)=-1$, where μ denotes the Möbius function. Using these observations we conclude that

$$\begin{aligned}\Phi_{mm_1}(x) &\equiv \prod_{d|mm_1,d<2p_1}(1-x^d)^{\mu(\frac{mm_1}{d})} \pmod{x^{2p_1}}\\ &\equiv \prod_{d|m}(1-x^d)^{\mu(\frac{m}{d})\mu(m_1)}\prod_{j=1}^{t}(1-x^{p_j})^{\mu(\frac{mm_1}{p_j})} \pmod{x^{2p_1}}\\ &\equiv \Phi_m(x)^{\mu(m_1)}\prod_{j=1}^{t}(1-x^{p_j})^{-\mu(mm_1)} \pmod{x^{2p_1}}\\ &\equiv \frac{1}{\Phi_m(x)}\prod_{j=1}^{t}(1-x^{p_j})^{\mu(m)} \pmod{x^{2p_1}}\\ &\equiv \frac{1}{\Phi_m(x)}(1-\mu(m)(x^{p_1}+\cdots+x^{p_t})) \pmod{x^{2p_1}}.\end{aligned} \tag{2}$$

From (2) it follows that, if $p_t\le k<2p_1$, then

$$a(mm_1,k)=c(m,k)-\mu(m)\sum_{j=1}^{t}c(m,k-p_j).$$

By Lemma 2.1 we have $c(m,k-p_j)=c(m,k-1)$, and therefore

$$a(mm_1,k)=c(m,k)-\mu(m)tc(m,k-1) \text{ with } p_t\le k<2p_1. \tag{3}$$

Since $\mu(m) = 1$, we let $q_3 < q_4$ be the smallest two prime divisors of m. Here we also required that $n \geq 8q_4$, which ensures that $p_t + q_4 < 2p_1$. Note that

$$\begin{aligned}\frac{1}{\Phi_m(x)} &\equiv \frac{(1-x^{q_3})(1-x^{q_4})}{1-x} \pmod{x^{q_4+2}} \\ &\equiv 1 + x + x^2 + \cdots + x^{q_3-1} - x^{q_4} - x^{q_4+1} \pmod{x^{q_4+2}}.\end{aligned} \tag{4}$$

Thus $c(m,k) = 1$ if $k \equiv \beta \pmod{m}$ with $\beta \in \{1,2\}$ and $c(m,k) = -1$ if $k \equiv \beta \pmod{m}$ with $\beta \in \{q_4, q_4+1\}$. This in combination with (3) shows that $a(m_1 m, p_t+1) = 1-t$ and $a(m_1 m, p_t + q_4) = t-1$. Since $\{1-t, t-1 | t \geq 1\} = \mathbb{Z}$, then $S(m; s, t) = \mathbb{Z}$ and the first result follows.

To prove $R(m; s, t) = \mathbb{Z}$. As before we may assume that $m > 1$ is square-free and $\mu(m) = 1$.

Let q_1, q_2 be primes such that $q_2 > q_1 > 2p_1$, $q_1 \equiv t \pmod{s}$ and $q_2 \equiv 1 \pmod{s}$ and put

$$\bar{m}_1 = \begin{cases} p_1 p_2 \cdots p_t q_1 q_2 & \text{if } t \text{ is even;} \\ p_1 p_2 \cdots p_t q_1 & \text{otherwise.} \end{cases} \tag{5}$$

Note that m and m_1 are coprime and that $\mu(\bar{m}_1) = 1$. Reasoning as in the derivation of (2) we obtain

$$\frac{1}{\Phi_{mm_1}(x)} \equiv \frac{1}{\Phi_m(x)}(1 - \mu(m)(x^{p_1} + \cdots + x^{p_t})) \pmod{x^{2p_1}} \tag{6}$$

and from this $c(\bar{m}_1 m, k) = a(m_1 m, k)$ for $k \leq 2p_1$. Reasoning as in the proof $S(m; s, t) = \mathbb{Z}$, we obtain $R(m; s, t) = \mathbb{Z}$. This completes the proof. $\square$

Remark: Since we do not need to consider the case $\mu(m) = -1$, so a proof a little easier than that given in [12] is obtained.

Acknowledgments: The author is supported by NSF of China (No. 10971072) and by the Guangdong Provincial Natural Science Foundation (No. 8151027501000114).

References

[1] G. Bachman, *Flat cyclotomic polynomials of order three*, Bull. London Math. Soc. 38 (2006), pp. 53-60.

[2] G. Bachman, *Ternary cyclotomic polynomials with an optimally large set of coefficients*, Proc. Amer. Math. Soc. 132 (2004), pp. 1943-1950.

[3] M. Beiter, *The midterm coefficient of the cyclotomic polynomials*, Amer. Math. Monthly, **71**(1964), 769-770.

[4] M. Beiter, *Coefficients in the cyclotomic polynomials for numbers with at most three distinct odd primes in their factorization*, The Catholic University of American Press, Washington 1960.

[5] L. Carlitz, *The number of terms in the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly, **73**(1966), 979-981.

[6] T.Y. Lam and K.H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly, **103**(1996), 562-564.

[7] H.W. Lenstra Jr., *Vanishing sums of roots of unity*, Proc. Bicentennial Cong. Wiskundig Genootschap, Vrije Univ., Amsterdam (1978), pp. 249-268.

[8] A. Migotti, *Zur Theorie der Kreisteilungsgleichung*, Sitzber. Math.-Naturwiss. Classe der Kaiser. Akad. der Wiss. 87 (1883), pp. 7-14.

[9] P. Moree, H. Hommersom, *Value distribution of Ramanujan sums and of cyclotomic polynomial coefficients*. arXiv: math.NT/0307352.

[10] J. Suzuki, *On coefficients of cyclotomic polynomials*, Proc. Japan Acad. Ser. A Math. Sci. 63 (1987), pp. 279-280.

[11] Chun-Gang Ji, Wei-Ping Li, *Values of coefficients of cyclotomic polynomials*, Discrete Mathematics, **308**(2008), 5860-5863.

[12] Chun-Gang Ji, Wei-Ping Li, Pieter Moree, *Values of coefficients of cyclotomic polynomials II*, Discrete Mathematics, **309**(2009), 1720-1723.

[13] Pieter Moree, *Reciprocal cyclotomic polynomials*, Journal of Number Theory **129**(2009), 667-680.

[14] Ravindranathan Thangadurai, *On the coefficients of cyclotomic polynomials*, in: Cyclotomic Fields and Related Topics (Pune, 1999), Bhaskaracharya Pratishthana, Pune, 2000, pp. 311C322.